谷歌搜索框XSS漫谈

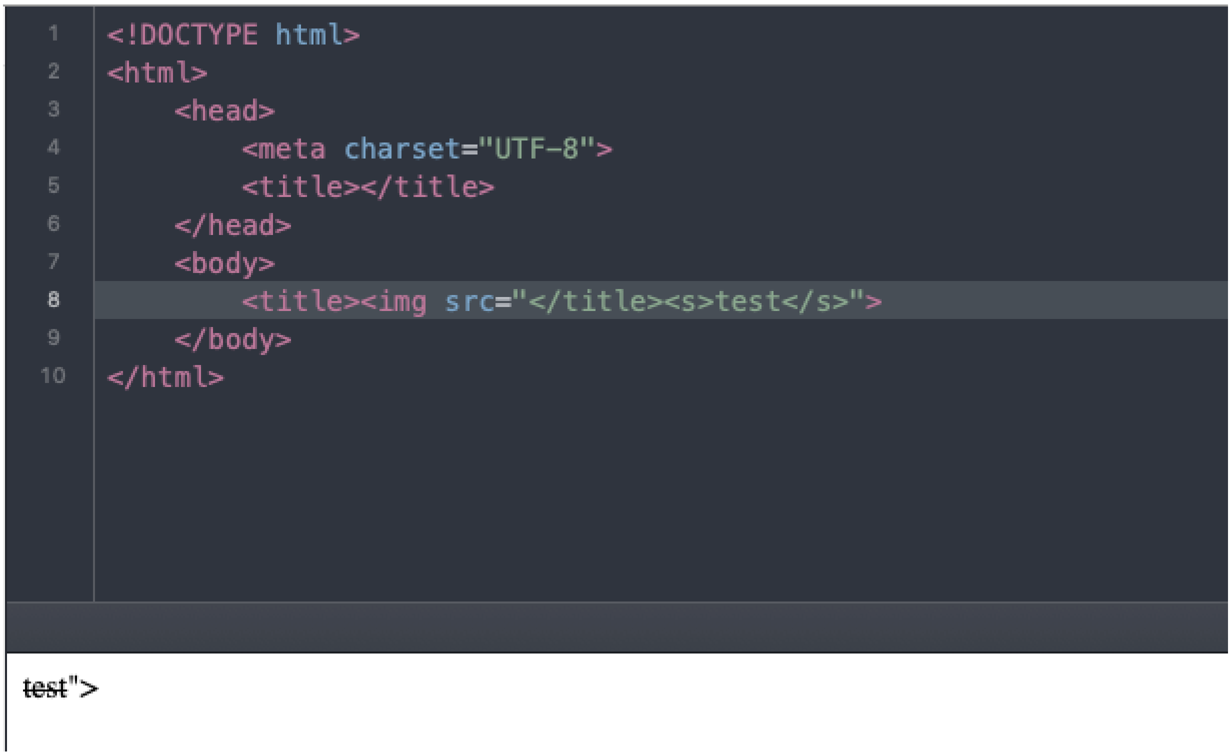
前几天看了谷歌搜索框的XSS，有一个视频讲的非常好 https://www.youtube.com/watch?v=gVrdE6g_fa8，这个视频不仅讲了该漏洞的原理，同时还说了mk如何来研究这个漏洞，以及告诉你一些挖掘此类漏洞的技巧。

这个漏洞的关键就是parser bug与差异。

何为parser bugs

parser bugs 指的是在解析某些“符合某种标准的文本”中出现的bug。在XSS漏洞中通常是，寻找后端parser与浏览器parser的区别。

还是我在 https://t.zsxq.com/biieAAA 这个帖子里举的例子：



看编辑器中的颜色就能看出，这个编辑器认为`</title><s>test</s>`是img标签的src属性，而实际上下方的浏览器渲染结果是，删除线被渲染出来，也就是`<s>test</s>`被渲染成了一个标签。

这就是典型的parser bug，编辑器中的html parser与浏览器的parser不相同，也就可能造成如`<s>`一样的不在白名单里的标签逃逸出过滤器，造成XSS漏洞。

js html parser api

谷歌这个案例中，mk寻找到了更为有趣的bug，就是js html parser api与浏览器parser的区别。虽然js和dom都在浏览器端执行，实际上内部是两个不同的项目，所以自然可能存在区别。

js中有哪些常见的html parser api?

1. 利用template元素

```
var template = document.createElement('template')
template.innerHTML = '<img src=1  onerror=alert(1)>'
template.content.children
template.content.children[0]
```

2. 利用DOMParser对象：

https://developer.mozilla.org/en-US/docs/Web/API/DOMParser

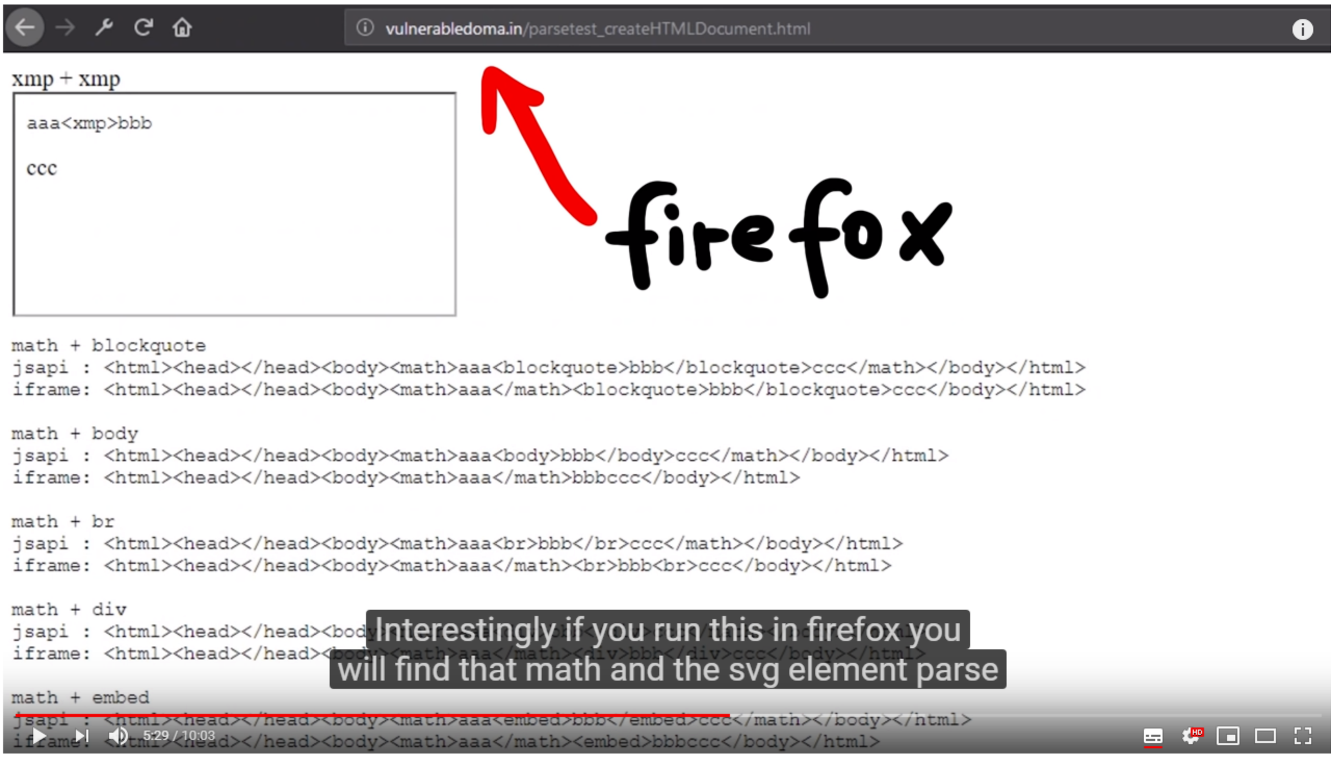
```
parser = new DOMParser();
doc = parser.parseFromString(stringContainingHTMLSource, "text/html");
```

3. 利用`DOMImplementation.createHTMLDocument()`方法

https://developer.mozilla.org/en-US/docs/Web/API/DOMImplementation/createHTMLDocument

```
function makeDocument() {
  var frame = document.getElementById("theFrame");

  var doc = document.implementation.createHTMLDocument("New Document");
  var p = doc.createElement("p");
  p.innerHTML = "This is a new paragraph.";

  try {
    doc.body.appendChild(p);
  } catch(e) {
    console.log(e);
  }

  // Copy the new HTML document into the frame

  var destDocument = frame.contentDocument;
  var srcNode = doc.documentElement;
  var newNode = destDocument.importNode(srcNode, true);

  destDocument.replaceChild(newNode, destDocument.documentElement);
}
```

mk编写了一个页面，fuzz出了浏览器dom渲染（使用iframe）与上述三个js parser的差异：



视频中可以看到，差异其实还是蛮多的。

chrome中是noscript、noembed标签带来了差异，firefox多了math和svg标签。

最后，也就是利用noscript标签，他成功打破谷歌搜索框的限制，制造了一个mxss。

参考阅读

漏洞的原理网上已经有文章说的比较清楚了，视频里也讲了，不太明白的可以自己再研究研究。这里我只是说下我的一些感想。

- 这篇文章讲了一部分原理 https://www.acunetix.com/blog/web-security-zone/mutation-xss-in-google-search/
- 视频作者给出的一个fuzz差异的脚本https://gist.github.com/LiveOverflow/dd3d09d17c8fc0460c7e9a337b501331